Remarks

Reconsideration of the application and allowance of all pending claims are respectfully requested. Claims 1-20 remain pending, including independent claims 1, 17, 18 & 20.

By this paper, independent claims 1, 17, 18 & 20 are amended to more clearly point out and distinctly claim the protocol of Applicants' invention. Support for the amended language can be found throughout the application as filed, for example, reference FIG. 3 and the supporting discussion thereof. No new matter is added to the application by any amendment presented.

Initially, Applicants respectfully request reconsideration of the 35 U.S.C. §112, second paragraph, rejection to claims 3, 7, 11 & 16 as filed. By this paper, these claims are amended to address each of the indefinite issues noted in the Office Action. These claims are believed to now particularly point out and distinctly claim the subject matter which Applicants regard as the invention, and thus, reconsideration of the rejection is requested.

Substantively, claims 1, 4, 6, 8, 12-15, 17, 18, & 20 were rejected under 35 U.S.C. §102(e) as being anticipated by Peyret et al. (U.S. Patent No. 5,923,884; hereinafter Peyret), while claims 2, 7, 10 &19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Everett et al. (U.S. Patent No. 6,575,372; hereinafter Everett), claim 16 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Hanel (UK Patent Application No. GB 2,314,948; hereinafter Hanel), claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Klingman (U.S. Patent No. 5,729,594; hereinafter Klingman), and claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of a textbook by B. Schneier, entitled "Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code NC" (hereinafter, Schneier). Each of these rejections is respectfully, but most strenuously, traversed to any extent deemed applicable to the amended claims presented herewith, and reconsideration thereof is requested.

Independent claims 1, 17 & 20 recite a method, device and computer program product, respectively, which implements a protocol for downloading application components from a server via a client to a chipcard. This protocol includes: delivering a secret key or Session Key by the sever to the client; loading into the server a sequence of commands to download an application component to the chipcard; generating a digital signature in the server using the secret key or Session Key by way of each command within the command sequence; transmitting the signed command sequence as a data packet to the client; unpacking of the data packet by the client and transmission of individual commands to the packet in sequence to the chipcard; and then checking the digital signature of the individual commands on the chipcard and executing the commands if the digital signature is correct.

In accordance with Applicants' protocol, downloading of application components is divided into stages. The first stage occurs only on the server, which ensure that not every command to download the application component is sent individually over the network connecting the server and client. This is achieved by an optimization protocol which bundles the individual commands to download the application component into command sequence and then send this command sequence as a data packet over the network. This reduces the time required for downloading application components over the network. In accordance with Applicants' protocol, each command within the command sequence is assigned a digital signature, and where appropriate, encrypted. This assures that only authenticated commands are accepted by the chipcard. Thus, the protocol meets security requirements for the transferred data via distributed systems, such as over the Internet.

The second stage occurs between the client and the chipcard and ensures that the data packet is unpacked and sent individually to a chipcard. The individual commands of the unpacked data packet are sent sequentially to the chipcard from the client. Thus, in accordance with Applicants' invention, intelligence is added to the client for receiving a data packet comprising a signed command sequence, and then unpacking the data packet and transmitting the individual commands in sequence to the chipcard. Independent claim 18 focuses on this aspect of Applicants' protocol, wherein a client is provided with the intelligence via a computer program product to execute the unpacking of the data packet comprising the signed command sequence and then transmit the individual commands thereof in sequence to the chipcard.

Applicants respectfully submit that the above-summarized protocol is simply not taught or suggested by the art of record, and in particular, by the applied documents.

With respect to the anticipation rejection, it is well settled that there is no anticipation of a claim unless a single prior art reference discloses: (1) all the same elements of the claimed invention; (2) found in the same situation as the claimed invention; (3) united in the same way as the claimed invention; and (4) in order to perform the identical function as the claimed invention. In this instance, Peyret fails to disclose various aspects of Applicants' invention as recited in the independent claims presented, and as a result, does not anticipate (or even render obvious) Applicants' invention.

Peyret discloses a system and method for loading applications onto a smartcard. FIG. 4 depicts a block diagram showing a system in accordance with Peyret's invention for loading an applet having use rights into a smartcard. The system may include the smartcard 20, a terminal 80, and a server 82. The smartcard may have an interface system 86 that may connect the smartcard to the terminal 80 using a corresponding interface 88. A second interface 90 may connect the terminal to the server 82 via interface 92. Thus, the smartcard may be connected, through the terminal, to the server.

A method of loading an application into the smartcard is described at Col. 7, line 43 – Col. 8, line 15 of Peyret. As described, an application is loaded from server 82 to smartcard 20 via the terminal. However, in the embodiment described by Peyret, terminal 80 simply comprises a pass-through or dumb terminal since there is no intelligent protocol at terminal 80 which facilitates the loading of the application from the server to the card. Peyret in fact describes the traditional prior art approach to downloading an application to a smartcard and hence has the disadvantages noted by Applicants in their Background of the Invention section of the specification.

Applicants respectfully submit that a careful reading of Peyret fails to disclose any teaching or suggestion of various aspects of their protocol for downloading application components from a server via a client to a chipcard. For example, Peyret does not teach or suggest any processing protocol between the sever and terminal (i.e., client) which would minimize data transfers between the server and the client. Further, there is no teaching or suggestion in Peyret that the terminal described therein is even able to read the content of the messages from the server. Rather, the Peyret terminal is simply a pass-through terminal. Peyret does not introduce the concept of transmitting a signed command sequence as a data packet from a sever to the client as recited by Applicants, nor the unpacking of the data packet by the client and then the transmission of individual commands within the packet in a sequence to the chipcard.

For the above-noted reasons, Applicants respectfully submit that independent claims 1, 17, 18 & 20 patentably distinguish over the teachings of Peyret. Each of these claims recites the transmission from the sever of a signed command sequence as a data packet as shown by Applicants in FIG. 3 of the present application. Further, each of these claims recites intelligence at the client for unpacking this data packet and then transmitting the individual commands bundled therein in sequence to the chipcard.

The Office Action fails to reference any teaching in Peyret for the above-summarized aspects of Applicants' intelligent protocol for transmitting a sequence of commands from the server to the chipcard. The Office Action references Col. 9, lines 50-57 only in connection with this protocol. These lines of Peyret discuss authentication of an applet code at the smartcard, and are not relevant to Applicants' claimed protocol for transmitting the signed command sequence as a data packet from the server, the unpacking thereof by the client, and the transmission of individual commands from the packet in sequence to the chipcard. Thus, Applicants respectfully submit that the Office Action fails to state a *prima facie* case of anticipation, or even obviousness, relative to the independent claims presented.

Reconsideration and withdrawal of the anticipation rejection based thereon is respectfully requested.

With respect to the obviousness rejections to various dependent claims, Applicants note that an "obviousness" determination requires an evaluation of whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art. In evaluating claimed subject matter as a whole, the Federal Circuit has expressly mandated that functional claim language be considered in evaluating a claim relative to the prior art. Applicants respectfully submit that the application of these standards to the claims at issue leads to the conclusion that the recited subject matter would not have been obvious to one of ordinary skill in the art based on the applied Peyret, Everett, Hanel, Klingman and Schneier reference.

Everett, Hanel, Klingman and Schneier are each cited in the Office Action for allegedly teaching various aspects of Applicants' dependent claims. Without acquiescing to the characterizations of these references and their alleged applicability to Applicants' dependent claims, Applicants note that none of the references are cited in the Office Action for teaching or suggesting Applicants' above-noted protocol for downloading application components from a server via an intelligent client to a chipcard. Thus, the dependent claims at issue are believed allowable for the same reasons as the independent claims from which they directly or ultimately depend, as well as for their own additional characterizations.

To summarize, Applicants respectfully submit that all claims are in condition for allowance and such action is requested. Each of the independent claims recites protocol for transmitting a signed command sequence as a data packet from a server to an intelligent client, which then unpacks the data packet and transmits individual commands in the packet in sequence to the chipcard. Applicants respectfully submit that this protocol, in the context of Applicants' recited technique for downloading application components from a server via a client to a chipcard, recites patentable subject matter over the applied art.

If a telephone conference would be of assistance in advancing prosecution of the subject application, Applicants' undersigned attorney invites the Examiner to telephone him at the number provided.

Respectfully submitted,

Kevin P. Radigan

Kevin P. Radigan, Esq.
Attorney for Applicants
Reg. No.: 31,789

Dated: October 05, 2004

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203
Telephone: (518) 452-5600
Facsimile: (518) 452-5579